The Databus

Newsletter of the Dayton Microcomputer Association®

Volume III (New Series), Issue 11 — **November 2012**

LEROY CLOUSER:

The NEAT® Scanning & Filing System

Tuesday, October 30, 7:00 P.M., 4801 SPRINGFIELD STREET

Click here for a map — free parking
All DMA General Meetings are free and open to the public — bring a friend!

NeatDesk®

NeatReceipts®

CONTENTS:

LEROY CLOUSER will speak to us this month about the Neat Desktop scanner and filing system. Make quick work of paper clutter with NeatDesk. First of all, what does a Neat scanning system do for you?

NeatDesk will scan your receipts, business cards, or documents at a speedy 24 pages per minute. Scan up to 50 pages at once – 1 or 2–sided, color or Black and White, single or multi-page. At home or on the go, Neat turns paper piles to organized digital files. Neat reads and extracts the information from whatever you scan. Receipts become digital records with vendors and amounts, business cards become digital contacts, and documents become fully keyword searchable.

Create tax or expense reports with your receipt data, or export to Excel, Quicken, or TurboTax. Sync your contacts with Outlook or Addres Book. Find what you need with a keyword, and organize it however you like.

The Dayton Microcomputer Association®, Inc.

Post Office Box 4005
Dayton, Ohio 45401

ESTABLISHED IN 1976, DMA is a group of Dayton–area professionals and hobbyists in the field of computing and information technology. General membership meetings are usually on the last Tuesday of each month. DMA has a number of Special Interest Groups (SIGs) in areas ranging from digital photography and geneology to the Linux operating system. Each SIG meets according to its own schedule. DMA is a member of APCUG and ASC. (Click on any of the logos — including our own — to go to that organization's Home Page.)

Officers and Board of Trustees

Association of Personal Computer User Groups

Submissions …

THE DATABUS welcomes compliments, complaints, suggestions, and especially articles. We can accept articles in ASCII, or as attachments in Microsoft Word or Works, Open Office Writer, Word Perfect, or even WordStar! No PDF files, please. Send e–mails to:

Editor@DMA1.org

All articles are subject to editing for spelling, grammar, usage, and space. Always retain a copy of your work, as THE DATABUS cannot be responsible for loss. When articles are of roughly equal quality, those by paid–up DMA members receive preference.

Hotel Wi–Fi Networks Installing Malware

by Sandy BERGER, CompuKISS
www.compukiss.com
sandy (at) compukiss.com

IF YOU ARE TRAVELING THIS YEAR, there is a new hacking scheme that you should be aware of. The Federal Bureau of Investigation is warning travelers to watch out for malware that comes through hotel Internet connections.

Here's how it works: When you get to a hotel and connect to the Internet through its wireless or wired Internet connection, you get a pop–up notifying you that you must update your Java in order to have the connection work. When you give your approval, malware is installed on your computer, giving the hackers access to your personal information. The malware also serves third–party advertisements to infected computers.

Bloomberg has recently reported that Chinese hackers have stolen private data from as many as 760 firms by hacking into the iBahn, a broadband and entertainment service that is offered to guests of hotel chains such as Marriott International Inc.

The advice offered by the FBI's Internet Crime Complaint Center (ISC3) includes:

- Carry out all software updates *before* traveling.
- Checking the author or digital certificate of any prompted update to see if it corresponds to the software vendor. (For example, does a "Microsoft" update really come from Microsoft?)
- Download software updates *directly* from the vendor's website.

I recommend skipping any software updates that you are offered when traveling and using an encrypted connection for handling e–mail when you are on the road. The way to do this depends on how you access your email when you travel.

Gmail is secure since it is encrypted. Other email, however, may not be encrypted. For instance, Time Warner's Road Runner Web Mail that you can use when you travel encrypts your user name and password, but not your e–mail itself. Other services may be different. You will want to investigate the service you are using. If you are not sure if your email is encrypted, you can use a free service called Mail2Web at www.mail2web.com
To use it you simply click on "Secure Login" then put in your e–mail address and password. (Make sure you don't just click "Check Mail" which gives you an unencrypted connection.)

If you are not traveling, you still need to keep your guard up. I recently received a very real-looking e–mail that was supposed to be from Order–update(at)amazon.com. [Editor's Note: I have disabled this link.] Since I often make purchases at Amazon, this piqued my interest. The message said that my Amazon order had been successfully canceled and gave a link to the order in question as well as to Amazon's Web site. I didn't want any orders canceled, so I read the entire e–mail. Then I hovered my mouse over the two links that supposedly went to Amazon and found that they went to some other

(Continued on page 4)

(Continued from page 3)

Web site. (This is a great way to check the links in an e–mail. Just remember that you only put your mouse over the link rather than actually clicking on it).

Remember that if you come across these or any other suspected hacking or phishing schemes, you can report them to the FBI's Internet Crime Complaint Center (ISC3) at www.ic3.gov This website also has great information and alerts for the latest scams.

You will be amazed by the sheer number of crime schemes that are floating around the Internet. There is everything from Ponzi and Pyramid schemes to Internet Extortion. So check out this Web site. Just as in real life, you have to be aware of the pitfalls to keep yourself safe. It's always good to follow the advice given by Sergeant Phil Esterhaus in Hill Street Blues. "Let's be careful out there."

How Do I Keep People From Finding Me on the Internet?

by Leo NOTENBOOM
http://articlesbyleo.com/
www.ask-leo.com

DO YOU WISH you could erase yourself from the internet? In other words, do you want to stop your name and information from showing up when people Google or search for you on the Internet? Sadly, you're not alone.

Not only is this disappointingly complex to do, ultimately … you can't.

What it boils down to is understanding how little control you have, what steps you can try, and how effective they may or may not be.

But first, you should know that prevention is the only real cure.

But even then it's not at all complete.

You need to assume that everything you place on the Internet will remain there forever, and will be viewed in the worst light possible. To clarify, it may not be there forever, and may not be viewed in the worst light possible, but that's the *safest* way to look at how what you say, do, and post in public might be used. You do have control over some of what goes up on the Web before it goes up, so exercise caution.

Still feel like posting those party photos?

(Continued on page 5)

(Continued from page 4)

How about the example we hear about all the time: someone losing a job or job offer because they spoke their mind in a public post, posted unflattering photos of themselves, or otherwise made public information about themselves that they never should have. Information that their employer or potential employer eventually found.

It happens all the time.

It happens to those who have the freedom of speech mentality: "I should be able to post and say and do whatever I want."

Absolutely. You should be able to. Go ahead. Post and say what you like. In most countries you have the right to say pretty much whatever you like. Just remember that freedom of speech does not mean freedom from consequences.

Because chances are you're not going to get it removed from the Internet once the day comes that you decide maybe it shouldn't be there.

Even preventing what you do and post may not be enough. What about other sources of information that relate to you?

You cannot control what others say or post about you. (Within the legal limits of harassment, libel and slander, of course, and even then within the limits of your own legal or justice system and your resources.) Been mentioned in a newspaper? Listed in publicly available records? Do you participate in discussion groups that are visible or archived publicly?

All of these are ways you can show up online. And there are plenty more.

And more than likely, all are places from which you probably can't remove yourself.

Still want to try? Here's what you can do:

Your first thought may be to try to get in touch with the search engine, but here's the fundamental problem: the search engine has nothing to do with it. Even though people may use the search engine to find the information, that information is not in the search engine itself. It's on one of the thousands of other sites on the Internet, and the search engine is merely in charge of finding it. The only way truly to remove yourself is to find each of those sites and ask them to remove the information that pertains to you. It's common to want to have Google staff remove you from its index. There are two problems: **1.** They won't. Google is a search engine, and its "job" is to report what can be found on other sites on the Internet. It's

(Continued on page 6)

simply showing you what's out there, but what's out there is not in their control. **2.** Google is not the only game in town. Google is perhaps the most popular, but there are literally thousands of search engines on the Internet. From Bing to Yahoo, to many medium and smaller niche search engines, there are more search engines than you could ever count. Even if you could get the Google people to remove you from their results, which you cannot, you'd still be faced with all those other search engines that might also be returning the same results that show your information on the internet.

Look out for a growing service area called "reputation management." These services will promise to remove you from the search results. They can't. If they tell you that they can, they're wrong. The information cannot been removed. The best that they can hope to accomplish is to push whatever it is you want to hide further down the results list when people use common search terms for you. At best it's simply somewhat harder to find … which may, or may not, be valuable to you.

It would be nice to think that you have control over the information that is placed on sites and services that you control on the web. But you don't. This is another way that this issue gets so complicated.

You might think that if you wanted to remove something about yourself that's been posted on your own website, all you need to do is exactly that — remove it. Problem solved.

Not so fast.

The "problem" is that there are other sites that take copies of the pages on your site and preserve them as a kind of historical record. Archive.org is a good example, but in fact there could once again be any number of sites archiving or duplicating information-and many of them are doing it illegally. You can certainly remove the information from *your* site, but you have no control over what these other sites do with the information that they've already captured and made publicly accessible.

So what can you do?

- Well, you can use the search engines yourself to see where all the information about you is, and then contact all of those sites (not the search engines) and ask them to remove it.
- You can use a reputation management service to try and "bury" your information, making it harder, but not impossible to find. If that's enough for you.

And that's about it. Once something is on the internet, you can pretty much plan on it being there for good.

In fact, it might be easier to change *you*: move, change your name, change all of your identifying information, and then make sure that as little of that new you as possible gets on the Internet.

But even then, you'll probably show up somewhere.

More Free Utilities to Clean Hijacked PCs

by Ira WILSKER

Ira is a member of the Golden Triangle PC Club, an Associate Professor at Lamar Institute of Technology, and hosts a weekly radio talk show on computer topics on KLVI News Talk AM560. He also writes a weekly technology column for the *Examiner* newspaper <www.theexaminer.com>. Ira is also a deputy sheriff who specializes in cybercrime, and has lectured internationally in computer crime and security.

WEB SITES MENTIONED IN THIS ARTICLE:

http://www.mcafee.com/us/downloads/free-tools/how-to-use-stinger.aspx
http://support.kaspersky.com/viruses/rescuedisk?level=2
http://www.avg.com/us-en/avg-rescue-cd
https://connect.microsoft.com/systemsweeper
http://www.superantispyware.com
https://www.emsisoft.com/en/software/eek/
http://www.malwarebytes.org
http://free.agnitum.com

HARDLY A WEEK GOES BY that I do not get a call from a friend or co-worker asking for help with a computer that had been hijacked by one of the thousands of variants of a type of malware generically known as "Rogue AntiVirus." Last weekend was busy for me in this respect in that I received several frantic calls for help on Friday, Saturday, and Sunday. All of the computers I was asked to clean had been totally hijacked by this rogue antivirus operating under the names "Vista AntiVirus 2012," "Windows 7 Antivirus," and "Microsoft Antivirus 2012."

While they all had different names, they all had the same *modus operandi* in that they infected a computer, displayed frequent popup windows alerting the user that the computer was heavily infected with viruses and spyware, offered to repair the problem for a fee, and totally took over the computer by not allowing most other programs to load. Often infecting the computer via an e–mail from a known acquaintance whose own computer had been hijacked and which sent out spam e–mail with a link that would load the malware, or by visiting a legitimate or rogue Web site that injects the malware via the Web browser, this rogue antivirus software is becoming more dangerous, and more difficult to remove. As has been written here before, this rogue software generally protects itself from detection and removal by neutralizing the installed security software on

(Continued on page 8)

(Continued from page 7)

the computer, and preventing other detection and repair software from executing. Most of the rogue software also blocks access to many of the websites with removal utilities, and prevents most programs on the computer from running by blocking almost all ".exe" files from opening.

What the user of the infected machine does not often see is that many of these rogue variants also disseminate their code to people whose e–mail addresses are in the user's address book (both webmail and computer based address books), Facebook and Twitter friends. This spamming of illicit code is typically in the form of friendly e–mails apparently from you to your e–mail buddies with a short polite message along with a link to a purloined Web site, which will automatically load the malware code onto their machines. Facebook and Twitter have also become major vectors used to promulgate this malware, as the rogue software will post short messages apparently from you, with links to the malware; anyone clicking on those links will be hijacked as well, and the process repeats geometrically. In addition to propagating itself, this rogue software also often adds the hijacked computers as "zombies" to a massive "bot" of computers used to send out spam e–mails for a fee, payable to the crook that started this spider web of malware and hijackings. In addition to the revenues from sending countless spam emails from the "bot" (network) of "zombies" (hijacked computers), the purveyors of this malware also generate substantial revenues by charging a fee, typically $29 to $69, often payable only by credit card, for the rogue software to "clean" the infected computer. If the unfortunate victim pays this extortion, not just will the rogue software not clean the computer, but will also often sell the credit card number (along with its expiration date, and CVV security code) on other illicit websites, typically resulting in massive fraudulent charges on the credit cards.

In the past, I have had great success using the free portable version of SuperAntiSpyware (www.superantispyware.com) to detect and remove the rogue antivirus infections. Using a clean computer, I download a fresh, updated copy of the portable version of SuperAntiSpyware to my USB flash drive, which I then take to the hijacked computer. I boot the infected computer into Safe Mode (F8), insert the flash drive, and run the SuperAntiSpyware, often in "full scan" mode. Once the machine has been cleaned, I use the "Repair" button on the bottom of the SuperAntiSpyware screen to undo many of the improper changes the malware had made to the computer. Because of its very frequent updating, ease of use, and high success rate, SuperAntiSpyware portable version is still my first choice to clean an infected computer. The problem is that in this very rapidly evolving cat–and–mouse game between the malware code writers and the security software companies, some of the recently released malware has become harder to detect and kill. I found this out last Friday when the normal battery of top–rated and updated malware detection and removal utilities that I carry on my flash drive (SuperAntiSpyware, Emsisoft Emergency Kit, and MalwareBytes) were unable to remove totally a persistent infection on a heavily compromised computer.

(Continued on page 9)

(Continued from page 8)

Knowing that a "Plan B" was necessary to defeat this stubborn malware, I went home to download some other utilities that I have used in the past to remove stubborn malware that resisted the most common and popular methods of cleaning. I downloaded the latest versions of McAfee's Stinger, Kaspersky Rescue Disk, AVG Rescue CD, and Microsoft Standalone System Sweeper Beta. I downloaded the McAfee Stinger to my flash drive, and created fresh CDs with the Kaspersky, AVG, and Microsoft utilities. Be sure implicitly to follow the directions provided by these software companies for creating the bootable CDs or bootable USB flash drives necessary to load and run the utilities.

Returning to the location of the hijacked desktop computer, I booted it into safe mode (F8), inserted my flash drive and ran the McAfee Stinger. While McAfee Stinger detects far fewer types of malware than many of the other utilities, it does an excellent job in detecting and killing some of the more stubborn infections, which it did on this victimized computer. After rebooting the computer, and rerunning the McAfee Stinger (it found no additional infections), there was very substantial improvement, but still some evidence of malware.

Then, I inserted my newly created bootable Kaspersky Rescue CD into the drive, and was required to press the F12 key in order to boot the computer with the bootable CD (some computers require F10 or F2 in order to select a "boot from CD or flash drive" option). Since booting with a CD does not load the infected copy of Windows that is on the hard drive, but instead loads a clean operating system from the CD (usually some form of Linux or WinPE), the malware cannot load and protect itself from detection and removal. The Kaspersky Rescue CD detected and removed the remainder of the malware, proving itself as a very viable method of malware removal. I removed the Kaspersky CD and inserted the Microsoft System Sweeper bootable CD, and rebooted the computer (F12). This Microsoft CD, very capable in its own right, did not detect any other malware on this computer, corroborating the fact that the computer was most likely clean of all forms of malware. If I still had any other problems, I know from past experience that the AVG Rescue CD, bootable the same way as the other CDs, has some very capable detection and system repair utilities which are often necessary to recover a badly damaged computer, but in this particular case, it was not necessary.

This badly infected and compromised computer had one of the major commercial security suites installed, but was still penetrated by the rogue antivirus, a common occurrence in that the rogue software is very well written by experts in security penetration. Rather than reinstall and update his current security software, which was near its expiration and renewal date, this computer owner wanted a different security suite than the one he had, in the hope that it would better protect his computer.

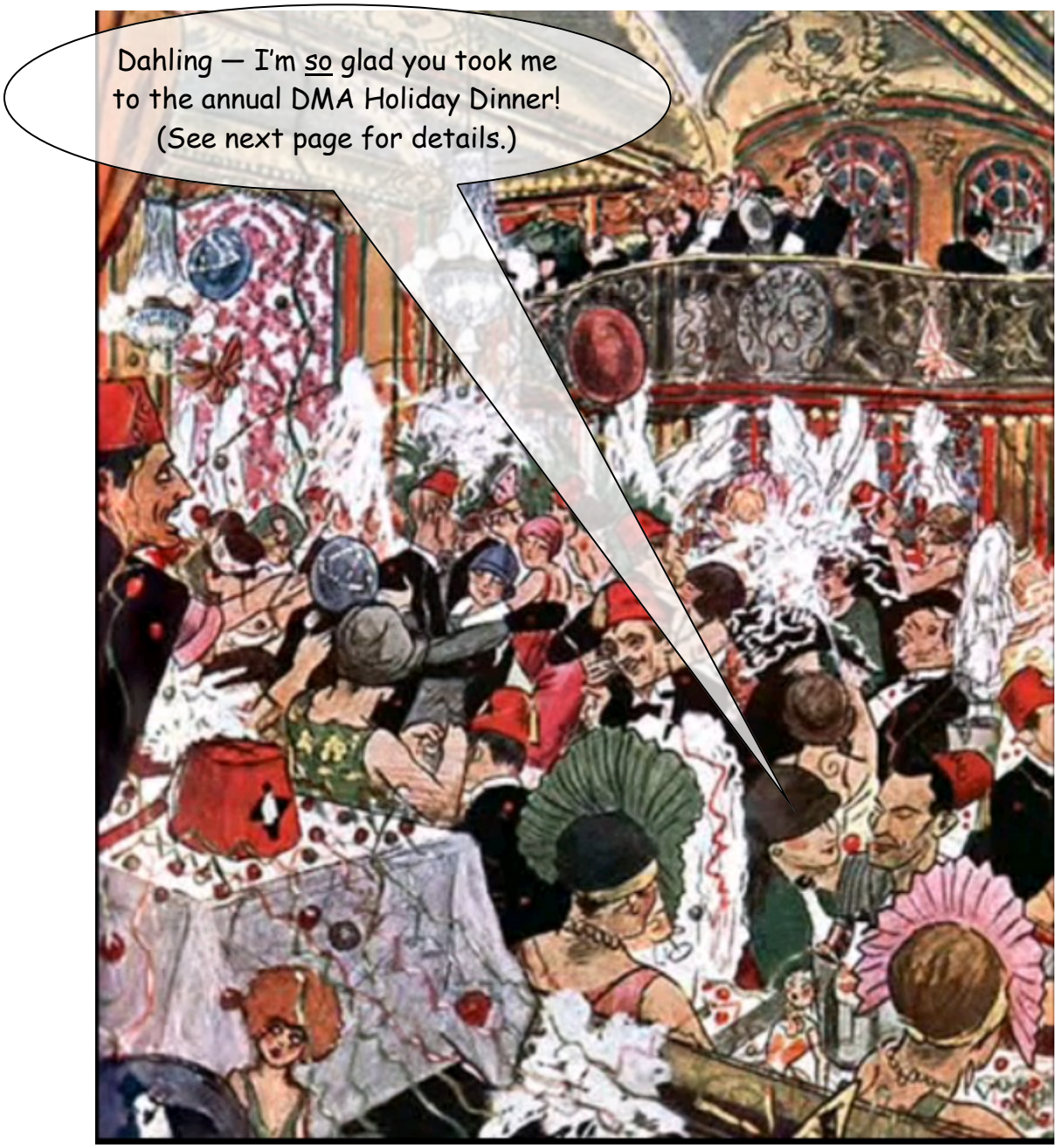
Whatever security software suite he would choose, it is absolutely imperative to install some comprehensive security suite *immediately* after cleaning the computer that

(Continued on page 10)

(Continued from page 9)

had been hijacked, as the security software that was previously installed was totally dead, killed by the malware in the earliest stage of the takeover, which left the computer vulnerable to the inevitable follow–on attacks. While there are several excellent commercial and free comprehensive security suites available, in this case the user decided to try one of the popular freeware security suites, Outpost (free.agnitum.com), rather than purchase another commercial product; that was his informed choice.

Now, when I am called upon to clean an infected computer, I include McAfee Stinger in the arsenal of utilities on my USB flash drive, and bring the three bootable CDs that I created (Kaspersky, AVG, and Microsoft), just in case they are needed.



Dayton Microcomputer Association

Events for December 2012

For additions or corrections, contact Dave Lundy

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Please note that our Web address (URL) has changed to DMA1.ORG						1 3:00-5:00pm Classic Computers
2	3 7:00pm DMA Board of Trustees	4 6:30pm Dayton Diode	5	6 6:30pm Genealogy SIG *Special Location*	7	8
9	10	11 6:00pm DMA Holiday Dinner	12 7:00pm Dayton Dynamic Languages Users Group	13	14	15 3:00-5:00pm Classic Computers
16	17 7:00pm Amateur Radio SIG 7:00pm Apple-Dayton SIG	18 7:00pm Software Development SIG	19	20 7:00pm Linux SIG	21 Winter Solstice	22
23	24	25 **Christmas Day**	26	27	28	29
30	31	Click anywhere on the DMA Calendar to go to the most recent update on our Web site.				

DMA Holiday Party!

Tuesday, December 11th at The Spaghetti Warehouse, 36 West 5th Street — click here for a map. Attitude adjustment (cash bar) at 6:00 P.M., dinner at 7:00.

DMA Membership Application/Renewal

PLEASE ALLOW UP TO THREE WEEKS FOR APPLICATION PROCESSING AND INTERNET SET–UP

Name: _____Birth date:_____/_____/_____
mo. day year

Associate Name: _____Birth date:_____/_____/_____
mo. day year

Address: _____

City: _____ State: _____ Zip: _____

Phone: (Home) (_____) _____-_____ (Work) (_____) _____–_____x_____

I wish to have my name and address published in the club roster: YES ❑ NO ❑

E–mail address: _____@_____

Name of DMA member who recruited me: _____ (only new regular memberships)

Are you a current or recent DMA Member? Yes ❑ No ❑ Change of Address only? ❑ Today's date: ____/____/____

If you are renewing, please give your Membership Number (from your membership card) _____

Type of Membership

Application is for: New Membership ❑ Membership Renewal ❑ Associate Membership* ❑

If applying for free student membership, please give school name and student ID number: Available only for students under 22 years old. (Student Members *cannot* vote in DMA elections.)

School Name: _____ Student ID#: _____

* A family or associate membership is an additional membership for a member of your immediate family or someone else who is living in the member's household. If this is a family or associate membership, give name of regular member:

Dues/Fees (Dues and Fees are subject to change without prior notice):

Membership (one year — New or Renewal)	1.) ❑ $25.00
Family or Associate Membership (must live at same address as regular member)	2.) ❑ $12.50
Free Student Membership for students under 22 yrs of age. (Student Members *cannot* vote in DMA elections.)	3.) ❑ FREE
Please assign me a user ID for E–mail and Usenet news access one–time setup fee for new E–mail accounts.	4.) ❑ $10.00
Total — Lines 1 and 2 (+ 4 if checked)	5) $_____

Make your check payable to Dayton Microcomputer Association, Inc. (DMA), and then send the check and application to:

PO Box 340402
Beavercreek, OH 45434–0402

DMA Use only: Membership # _____

Exp. Date: _____/_____/_____

Processed by: _____

REV: 26 June 2011

❑ Cash
❑ Check

Check # ____

Click here to pay your dues using PayPal. Simplified Membership Form, too!